INFORMATION ACCESS MANAGEMENT PROCEDURES

1. Information Access Management

The Los Angeles County Department of Mental Health (LACDMH) Chief Information Officer or his/her designee must work with System Managers/Owners, LACDMH Managers and Supervisors, and LACDMH Human Resources Bureau to develop information access procedures and to coordinate those activities necessary to implement the information access procedures.

The System Owners/Managers must ensure that appropriate physical safeguards and technical security policies are established and enforced. The System Owners/Managers must also ensure compliance with these polices is verified in such a manner and frequency that the purpose of this policy is demonstrably accomplished.

2. Elements

The information access management policy must include the following elements:

A. Access authorization
B. Access establishment and modification
C. Supervision of Workforce Members and others who do not have authorized access but work in locations where electronic data might be accessed.

3. Access Authorization

A. LACDMH must implement a role-based procedure specifying how a person is granted authorization to access confidential and/or sensitive information. LACDMH must also specify in writing who may authorize such access, for what purposes access can be authorized, and the procedures for approving and documenting the access authorization. The specification must include how and when to modify or cancel such access and procedures for communicating such changes to appropriate people and systems. These specifications must also establish limits on access to confidential and/or sensitive information based on the role(s) of the person (for example, a treatment provider generally needs access to health information only for people they are treating; a billing person needs only sufficient information to bill for work done, not full patient records, etc.). Access authorization must specify what authorized people may do with confidential and/or sensitive information - such as use (read), create, modify, and remove (delete).

B. The authorization criteria must include required levels of training and training certification requirements commensurate with the level of access. The access level must be established by a single point of approval, the System Manager/Owner or designee, and may be for a limited period of time. Renewal or a change of access level must require re-evaluation of access needs and may require continued or additional training.

4. Access Establishment and Modification

System Managers/Owners must specify in writing how to establish the access authorized. This must include specifying who is responsible for establishing the access, the procedures to be followed and how the granting of access must be documented.

System Managers/Owners must specify how to modify an access authorization including how to cancel an authorization. This includes who is responsible for establishing the change in authorization, the process for changing the authorization, and the process for documenting the changing of access.